IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

SECURITYPROFILING, LLC, Plaintiff/Counterclaim-Defendant, v. TREND MICRO AMERICA, INC. and TREND MICRO INCORPORATED, Defendants/Counterclaim-Plaintiffs.	§ § § § § § § § § §	Civil Action No. 3:17-CV-1484-N

DEFENDANTS' OPENING CLAIM CONSTRUCTION BRIEF

TABLE OF CONTENTS

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF AUTHORITIES

Page(s)

Cases

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Statutes

I. INTRODUCTION

The parties' claim construction disputes raise two primary issues: (1) whether Plaintiff may broaden the claims by resorting to a hodgepodge of extrinsic sources and disregarding (if not flatly contradicting) the intrinsic record concerning its purported invention and (2) whether generically claimed "code for" performing recited functions (and a few similarly generic terms) are computer-implemented means-plus-function terms requiring an algorithm—a threshold question that stands to dispose of five of the six patents and all but one claim in this case.

As to the first issue, the underlying purpose of claim construction is to interpret the claims as a matter of law in order to define and assist the jury in understanding their scope. Consistent with that purpose, Trend Micro, Inc. and Trend Micro America, Inc. (collectively "Trend Micro") proposed constructions derived from the intrinsic evidence. In contrast, SecurityProfiling, LLC ("SecurityProfiling") seeks to unduly broaden its claims primarily by piecing together flawed or otherwise improper extrinsic evidence. SecurityProfiling's motive for doing so is clear as it tries to read the claims on current technology that was never intended for the purported inventions—particularly computer and network security systems such as antivirus software that do not rely upon "vulnerability" information to defend against attacks.

As to the second issue, SecurityProfiling has asserted claims that include numerous generic "code for" elements that recite only functional language. The Federal Circuit has made clear that (1) such elements should be construed as means-plus-function terms and (2) if the specification does not disclose an algorithm for performing the recited function, the claim is invalid as indefinite. *See Williamson v. Citrix Online, LLC*, 792 F.3d 1339, 1349–50 (Fed. Cir. 2015). Application of this Federal Circuit authority to the claims is dispositive, as SecurityProfiling has not (and cannot) identified an algorithm for any of these terms.

II. LEGAL STANDARD

It is well-settled that, in interpreting an asserted claim, the court should look first to the intrinsic evidence of record, i.e., the patent itself, including the claims and specification, which is the most significant source of the legally operative meaning of disputed claim language. *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996). In addition, a court may rely on extrinsic evidence, such as dictionaries and treatises, to shed light on the claimed technology. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1317 (Fed. Cir. 2005).

Following *Philips*, the Federal Circuit has also made clear that "the specification is always highly relevant to the claim construction analysis and is, in fact the single best guide to the meaning of a disputed term." *Trustees of Columbia Univ. v. Symantec Corp.*, 811 F.3d 1359, 1363 (Fed. Cir. 2016). The claims "are part of a fully integrated written instrument, consisting principally of a specification that concludes with the claims" and "[t]he only meaning that matters in claim construction is the meaning in the context of the patent." *Id.* at 1363-64 (A "specification may define claim terms by implication such that the meaning may be found in or ascertained by a reading of the patent documents."). Accordingly, it has "recognized that when a patent 'repeatedly and consistently' characterizes a claim term in a particular way, it is proper to construe the claim term in accordance with that characterization." *See GPNE Corp. v. Apple Inc.*, 830 F.3d 1365, 1370 (Fed. Cir. 2016) (affirming construction of "node" to be a "pager …"). Trend Micro's constructions discussed herein are guided by these principles.

For certain limitations, a claim term "can operate as a substitute for 'means' in the context of § 112, para. 6" where it provides only "a generic description for software or hardware that performs a specified function." *Williamson*, 792 F.3d at 1349-50. Under *Williamson*, if the claim term does not denote a "sufficiently definite" structure for performing the function, it should be construed under § 112, ¶ 6. *Id.* at 1348. Pursuant to § 112, ¶ 6, a means-plus-function claim "shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof."[1] A term claimed in means-plus-function form must satisfy the definiteness requirements of § 112, ¶ 2, which require that the specification "particularly point out and distinctly claim" the subject matter of the invention. *Blackboard, Inc. v. Desire2Learn, Inc.*, 574 F.3d 1371, 1382 (Fed. Cir. 2009).

III. <u>BACKGROUND OF THE PATENTS-IN-SUIT</u>

The patents-in-suit are generally directed to methods and systems for identifying vulnerabilities associated with particular devices (*e.g.*, various computers located in a computer network) and detecting attacks that attempt to exploit those vulnerabilities. The underlying invention of U.S. Patent Nos. 8,266,699 ("the '699 Patent"); 8,984,644 ("the '644 Patent"); 9,100,431 ("the '431 Patent"); 9,117,069 ("the '069 Patent"); 9,118,708 ("the '708 Patent"); and 9,225,686 ("the '686 Patent") (Dkt. 1, Exs. A-F) (collectively, "the Patents-in-Suit") purported to provide a software application for remediating vulnerabilities (through patches, policy setting, and/or configuration options) by collecting information about the current configuration of the devices on the network and checking those configurations against a list of known vulnerabilities identified by software manufacturers or others in the industry to determine which devices had actual vulnerabilities. 2:29-47; 4:54-58.[2] Then, a user could select between remediation options to eliminate an identified vulnerability (*e.g.*, updating a device's outdated software). 5:64-6:10.

The patents also purport to permit existing network security products, such as firewalls, to access the information about device configurations and vulnerabilities via a Software

[1] Prior to the AIA's enactment in 2011, means-plus-function claims were governed under 35 U.S.C. § 112, ¶ 6. Post-AIA, the provision has been renamed to 35 U.S.C. § 112(f). Despite this name change, the substance of the statute has not been altered. Since claim terms must be interpreted as of the purported time of the invention, the parties have agreed that Pre-AIA § 112, ¶ 6, rather than § 112(f), applies here and will be referred to consistently herein.

[2] References to the specification are from the '644 Patent (Dkt. 1, Ex. B) unless noted otherwise.

Development Kit (SDK) to make security-related decisions following detection of an attack. 5:17-25; 3:59-4:21. The SDK similarly allowed for the same remediation of actual vulnerabilities following detection of an attack as discussed above. 4:41-53. The shared specification of the Patents-in-Suit primarily draws from SecurityProfiling's product marketing materials that were originally filed within a Provisional Application. As would be expected from marketing materials, the specification does not include detailed descriptions about the products and/or purported inventions as would be necessary for the functional claiming utilized here.

IV. **DISPUTED CLAIM CONSTRUCTIONS**

A. **"vulnerability" (Claim Term 1 – see Ex. 1-A at A8)**

The parties agree that a vulnerability is a condition that "can be exploited by an attack." Trend Micro's construction clarifies that it is a device configuration that is susceptible to such an attack, which is confirmed by the claims, specification, and contemporaneous extrinsic evidence. In contrast, SecurityProfiling proffers a jumble of non-contemporaneous extrinsic evidence, introducing vague and redundant language, to unduly broaden its claims.

It is long-established in the field that a vulnerability is tied to a device's configuration (for example, an operating system or the version of software installed). As the National Institute of Standards and Technology (NIST) explained in 2002, a "vulnerability" is a misconfiguration "in an operating system or other system software or application software component." *See* Ex. 1-B at A79; *id.* at A52 ("A vulnerability scanner . . . will identify a host's operating system and active applications and then compare these with its database of known vulnerabilities."). The claims and specification consistently use the term in this manner, describing vulnerabilities as defined by device configurations. Moreover, the extrinsic evidence (including SecurityProfiling's non-contemporaneous evidence) is in accord.

Claim Language: The claims make clear that a "vulnerability" is based on a particular device configuration that can be exploited by an attack. For example, Claim 1 of the '644 Patent expressly recites that a device "configuration" determines if "devices [are] actually vulnerable to at least one actual vulnerability." *See* '644 Patent, Claim 1 ("determining that the plurality of devices is actually vulnerable to at least one actual vulnerability based on the identified at least one configuration"). Claims 1 and 15 of the '431 Patent similarly utilize information derived from devices to determine whether an "attack" against a device can "take[] advantage of the at least one vulnerability."[3] No other claim uses the term in a manner inconsistent with this. *See In re Rambus Inc.*, 694 F.3d 42, 48 (Fed. Cir. 2012) (construing claim term consistently across related patents); *Omega Eng'g, Inc. v. Raytek Corp.*, 334 F.3d 1314, 1334 (Fed. Cir. 2003) ("[U]nless otherwise compelled . . . the same claim term in the same patent or related patents carries the same construed meaning."). As the claims make clear, it is a particular device configuration (*e.g.*, an outdated version of an operating system or software application that has yet to be patched or updated) that defines a vulnerability. Indeed, each vulnerability must be associated with a device configuration for the claimed processes to work.

Specification: The specification is similarly clear that a vulnerability is tied to a particular device configuration (*e.g.*, an operating system or program that needs to be updated). SecurityProfiling's disclosure relies primarily upon a "Security server 135" to collect device configuration information to determine whether vulnerable software is present on any devices and if it has been remedied by a patch or software update. *See* 4:4-12 ("Security server 135 . . . determine[s] whether the destination computer 137 has the vulnerable software installed, and whether the vulnerability has been patched on computer 137, or whether computer 137 has been

[3] As will be discussed more fully below with respect to the "occurrence" and "attack" terms, it is clear from the claims that "attacks" are directed against "devices" as well. *See supra*, IV.F.

configured so as to be invulnerable to a particular attack."). "Security server 135" accomplishes this by comparing (1) "the software installed on those devices, their configuration and policy settings, and patches that have been installed" to (2) "a regularly updated list of security vulnerabilities in software for a wide variety of operating systems." 2:32-39.

Thereafter, the server utilizes the "targeted machine's configuration to determine" whether it is vulnerable to a particular attack. *See* 11:20-24 ("automatically cross-reference the threat identifier with the targeted machine's configuration to determine if it is actually vulnerable to that threat"). Accordingly, the vulnerabilities utilized by "Security server 135" must be associated with a particular device configuration and/or software installation (such as a particular operating system or software program version) in order for the platform to make an effective classification or determination of the vulnerability. *See* 5:1-6 ("When a vulnerability is newly discovered in software that exists in subnet 130, administrators can immediately see whether any devices in subnet 130 are vulnerable to it, and if so, which ones. . . . [R]emediation can be selectively applied to only those devices subject to the vulnerability"). The specification repeatedly and consistently describes vulnerabilities in connection with a device configuration and should therefore be construed accordingly.[4] *See GPNE*, 830 F.3d at 1370 ("when a patent

[4] *See, e.g.*, 2:63-3:11 ("software installation status and configuration information" sent to security server and combined with "vulnerability and remediation data"); 3:12-26 (same); 5:63-6:10 (vulnerability remediation options relevant to "device or machine's particular configuration or status"); 7:5-20 ("information describing the operating system, software, and patches installed on the device(s), as well as the configuration thereof" is stored along with "data describing vulnerabilities of available software"); 8:42-52 ("cross-references the threat's identifier with the target's configuration" to determine "if the machine is vulnerable"); 11:46-53 ("cross-reference the threat's identifier with the target's configuration" to determine "if the machine is vulnerable"); *id.* ("cross-references the threat with the machine's existing OS, application, and patch configuration" to determine "if the machine is vulnerable"); 15:4-8 ("cross-references the threat with the machine's configuration profile"); 16:15-20 (describing "each computer's configuration profile"); 19:28-32 ("cross-references the threat's identifier with the target's configuration" to determine if the device "is vulnerable to the attack.").

'repeatedly and consistently' characterizes a claim term in a particular way, it is proper to construe the claim term in accordance with that characterization").[5]

Extrinsic Evidence: The parties' extrinsic evidence similarly supports Trend Micro's construction. As noted above, NIST has long defined a vulnerability in terms of a device's configuration (or misconfiguration) and installed software that leaves the device vulnerable to exploitation. *See* Ex. 1-B at A79, A52. The Trend Micro glossary cited by SecurityProfiling similarly confirms that vulnerabilities are tied to a device's configuration and installed software. *See* Ex. 1-C at A135 (vulnerabilities are "found in programs and operating systems leaving computing systems open to malware and hacker attack").[6]

In contrast, SecurityProfiling's construction appears to be derived solely from extrinsic evidence but picks and chooses words from multiple sources with no single source supporting the construction. Moreover, SecurityProfiling's evidence is improper because it (1) is not contemporaneous in time to the purported invention and (2) cites to documentation from Trend Micro's current website (referring to the accused products).[7] SecurityProfiling's construction

[5] *VirnetX, Inc. v. Cisco Sys., Inc.*, 767 F.3d 1308, 1318-19 (Fed. Cir. 2014) ("secure communications link" required both "data security and anonymity" because not a single embodiment provided "data security but not anonymity"); *Wi-LAN USA, Inc. v. Apple Inc.*, 830 F.3d 1374, 1382 (Fed. Cir. 2016) ("specification's consistent references to multiple 'specified connections' . . . weigh[s] in favor of a construction excluding embodiments where the intermediary node is capable of maintaining only one 'specified connection.'"); *Intellectual Ventures I LLC v. Capital One Bank*, 792 F.3d 1363, 1372 (Fed. Cir. 2015) (The "specification consistently describes the machine readable instruction form as a hard-copy document and thus [the construction] in no way contradicts the plain meaning of the claim language.").

[6] SecurityProfiling's "dictionary.com" definition is unhelpful and is only directed to the fact that the vulnerability "can be exploited by an attack" which is not in dispute here (while also providing a definition not at the time of invention). *See* Ex. 1-D at A138.

[7] *See Jeneric/Pentron, Inc. v. Dillon Co.*, 205 F.3d 1377, 1380 (Fed. Cir. 2000) ("To determine claim meaning," courts may consult "at times ***extrinsic evidence to discern the scientific and technological context at the time of invention***." (emphasis added)); *see also Brookhill-Wilk 1, LLC. v. Intuitive Surgical, Inc.*, 334 F.3d 1294, 1299 (Fed. Cir. 2003) (refusing to consider extrinsic evidence because it was "not contemporaneous with the patent"); *SRI Int'l v.*

results in an overly broad recasting of what was purportedly invented with redundant and vague wording that only will complicate issues for a jury. This construction appears drawn to remove the actual meaning from the term to expand coverage to antivirus scanners or other systems that do not utilize device vulnerability information for defending against attacks. Unlike Trend Micro, SecurityProfiling's construction disregards the intrinsic evidence and should be rejected.

B. "intrusion prevention system" (Claim Term 2 – see Ex. 1-A at A8)

The parties largely agree on the definition of an intrusion prevention system (IPS), but SecurityProfiling omits two key aspects of the term: that the IPS (1) takes actions in "real time" and (2) monitors, processes, and drops network traffic "packets." Both of these are fundamental to the purpose and operation of an IPS as understood in the art and used in the patents here.

First, that the specification and claims make clear that the IPS processes and prevents exploits in "real-time." The specification's sole IPS embodiment explicitly discloses that malicious packets are dropped "in real-time." *See* 20:7-9 ("commanded in ***real-time*** to drop the malicious packets"); *see also* 19:34-36 ("***immediately drop*** the exploit packets"); 19:8-10 ("IPS may be provided that provides intelligence, accuracy, ***real-time prevention***") (emphasis added). This is reinforced by the specification's description of the IPS that notes "attacks are accurately identified and mitigated ***before*** they reach their targets," which is impossible unless malicious packets were detected and dropped in "real-time." *See* 19:43-45 (emphasis added). The claims likewise make clear that the IPS's role is to "prevent[] advantage being take of actual vulnerability," which cannot be achieved without real-time action upon detection of an occurrence. *See* '644 Patent, Claim 2. Indeed, an IPS must process network traffic and drop

Matsushita Elec. Corp. of Am., 775 F.2d 1107, 1118 (Fed. Cir. 1985) ("It is only ***after*** the claims have been ***construed without reference to the accused device*** that the claims, as so construed, are applied to the accused device to determine infringement.") (emphasis in original).

malicious packets in real-time to accomplish their claimed function, as permitting delivery of malicious packets to a networked device does not prevent an intrusion, it permits one.

Second, the intrinsic record similarly supports that the IPS monitors, processes, and drops network traffic "packets." For example, in the '069 Patent, an "occurrence ***packet***" is detected and prevented by the IPS (or other mitigation technique). *See* '069 Patent, Claim 2 (emphasis added). The remaining asserted claims are not inconsistent. *See, e.g.*, '644 Patent, Claims 2, 3; '686 Patent, Claims 4, 14; *see also Rambus*, 694 F.3d at 48 (construing claim term in a uniform manner across related patents); *Omega Eng'g*, 334 F.3d at 1334 (same). Trend Micro's construction is likewise grounded in the only IPS embodiment within the specification, which states in relevant part "if the destination IP is vulnerable to the attack, the in-line Sensor is commanded in real-time to ***drop the malicious packets***." 20:7-9; 19:34-36 ("If the destination IP is vulnerable to the attack, the in-line Sensor is commanded to immediately ***drop the exploit packets***—preventing the attack") (emphasis added). *See Phillips*, 415 F.3d at 1316 (claims construed based on "what the inventors actually invented"); *see also GPNE*, 830 F.3d at 1370; *VirnetX*, 767 F.3d at 1318. The inclusion of "packets" in Trend Micro's construction clarifies the meaning of an IPS and is supported by both the claims and the specification.

Finally, the extrinsic evidence supports Trend Micro's construction. SecurityProfiling's IPS product literature, which purportedly forms the basis of the invention and was filed with the Provisional Application, is consistent with the specification. *See, e.g.*, Ex. 1-E at A143-A144 ("If the destination IP is vulenrable [sic] to the attack, the Inline Sensor is commanded in real-time to drop the malicious packets") ("Benefits: Attacks are accurately identified and mitigated before they reach their targets"). In contrast, SecurityProfiling cites to online sources that are not contemporaneous in time to the purported invention and are improper. *See Jeneric/Pentron*, 205

F.3d at 1380. Regardless, the definitions support both disputed aspects of Trend Micro's construction, explicitly describing the basic IPS function of dropping malicious packets in real-time. *See* Ex. 1-F at A146 ("an IPS can drop malicious packets"); Ex. 1-G at A150 ("Dropping the malicious packets," the IPS "must also ***work fast*** because exploits can happen in ***near real-time***"); Ex. 1-H at A154 ("intrusion prevention systems also have the ability to ***take immediate action***" and "might drop a packet that it determines to be malicious").

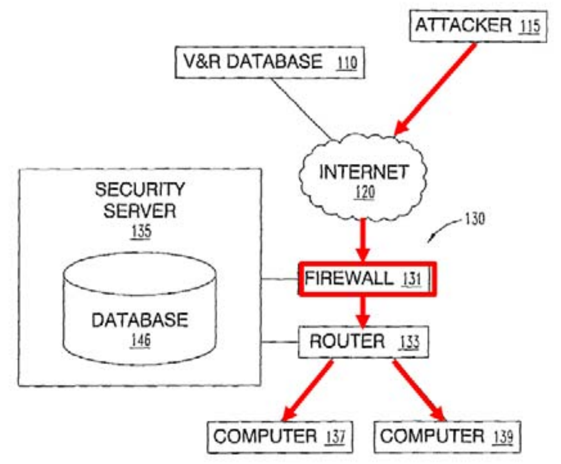
Again, SecurityProfiling's construction seeks to expand its purported invention beyond the intrinsic record, while trying to potentially equate intrusion prevention with unrelated security systems, such as antivirus scanners. Thus, Trend Micro's construction should be adopted, as it is more accurately grounded in the intrinsic and extrinsic record.

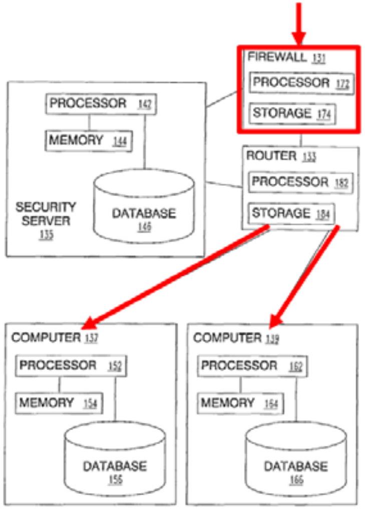
C. "firewall" (Claim Term 3 – see Ex. 1-A at A8)

The parties also generally agree on the construction of "firewall." However, SecurityProfiling has improperly removed "all" from the construction requiring "***all*** information" to pass through the firewall. SecurityProfiling's suggestion that "all" traffic entering a network need not flow through a firewall is contrary to the established meaning and fundamental purpose of a firewall and the patents' consistent usage of the term throughout their specifications.

The common meaning and basic purpose of a "firewall" is to act as a gateway or barrier to a network that prevents external computers from communicating directly to any computers behind the network's firewall by requiring all information to first pass through it. As a contemporaneous industry dictionary by Microsoft explains, a "firewall prevents computers in the organization's network from communicating directly with computers external to the network and vice versa. Instead, ***all communication*** is routed through" the firewall's proxy server. *See* Ex. 1-I at A158-A159. This is consistent with both parties' proposed constructions, which note that the firewall "acts as a barrier." Moreover, the glossary SecurityProfiling itself cites confirms a firewall's established purpose as "a barrier through which ***all information*** passing between the networks and the external systems must travel." *See* Ex. 1-C at A133 (emphasis added). In its final construction, however, SecurityProfiling excises "all" from this definition. *See id.*

SecurityProfiling's omission is similarly contrary to the intrinsic record, which describes a conventional firewall acting as a barrier that monitors all traffic at the perimeter of a network. *See* 10:11-15 ("These strategies generally call for network managers to lock down core servers, and monitor/scan/filter ***all incoming and outgoing traffic at the network perimeter*** with several network security products such as antivirus and ***firewalls*** . . . .") (emphasis added); *see also* 4:19-21 ("firewall 133 drops or rejects the connection request 211 as is understood in the art"); Figs. 1 and 2 (annotated below illustrating all network traffic passing through the firewall).

<table>
<tr><th>'644 Patent, Fig. 1 (annotated)</th><th>'644 Patent, Fig. 2 (annotated)</th></tr>
<tr><td>


</td><td>


</td></tr>
</table>

Nothing in the specification departs from this established understanding of firewalls.[8] Accordingly, because both the extrinsic and intrinsic record supports Trend Micro's construction, "all" information should be adopted over SecurityProfiling's unnecessary omission.

[8] SecurityProfiling attempts to depend on Trend Micro's recent (and non-contemporaneous) product documentation for support. Dkt. 88 at 2. However, this reliance on the accused products is both improper (see *SRI Int'l*, 775 F.2d at 1118) and irrelevant to its construction beyond demonstration that its removal of "all" from its construction is contrary to its own cited evidence.

D. "remediation technique" (Claim Term 4 – see Ex. 1-A at A8)

The parties agree that a "remediation technique" is "an action that corrects a vulnerability." However, the parties disagree as to other aspects of the construction. Particularly, SecurityProfiling (1) denies that "vulnerabilities" in the claimed method are associated with "devices;" (2) unnecessarily shoehorns a litany of example techniques into its construction; and (3) adds that remediation techniques may vaguely "counteract" a vulnerability.

First, the asserted claim of the '699 Patent is clear that each vulnerability is directed to and associated with one or more devices. *See* '699 Patent, Claim 7 ("a database that associates a plurality of ***device vulnerabilities*** to which computing ***devices can be subject***) (emphasis added). Accordingly, a "vulnerability" that is ultimately remediated need be actually "on a device." The specification also makes clear that remediation techniques are applied to devices to correct a vulnerability. *See* '699 Patent, 4:61-67 ("the remediation technique(s) are applied (1) to the machine that was attacked, (2) to all devices subject to the same vulnerability (based on their real-time software patch, policy, and configuration status), or (3) to all devices to which the selected remediation can be applied.");'699 Patent, 5:15-20 ("the remediation can be selectively applied to only those devices subject to the vulnerability").

Second, Trend Micro more clearly defines the term than SecurityProfiling, who shoehorns a variety of open-ended examples into its construction. *See, e.g.*, '699 Patent, 5:1-5.[9] It is unclear why SecurityProfiling deems these necessary and not included with "making changes to a device" in Trend Micro's construction (*e.g.*, "installation of a patch," device

[9] *See also Cisco Sys., Inc. v. Teleconference Sys., LLC*, No. 09-cv-01550, 2011 WL 5913972, at *8 (N.D. Cal. Nov. 28, 2011) ("The Court agrees that providing such an unexhausted list of examples would not assist the jury and could cause some confusion."); *Hitachi Consumer Elecs. Co. v. Top Victory Elecs. (Taiwan) Co.*, No. 2:10-cv-260, 2012 WL 5494087, at *12 (E.D. Tex. Nov. 13, 2012) (list of examples in construction "unhelpful" and "likely to confuse the jury").

configuration and registry changes, "closing of open ports on the device," etc.).[10] *See id.* These lengthy examples will not help a jury, as they include terms vague enough to themselves require construction (*e.g.*, "policy setting," "configuration option"). Trend Micro's construction is supported by the intrinsic evidence, is more helpful to the jury, and should be adopted.

Third, SecurityProfiling adds that remediation "counteracts" vulnerabilities in addition to "correcting" them, which is both unnecessary and unwarranted by the record. It is also unlikely to assist a jury's understanding, as a vulnerability is a condition of a computing device and it is unclear what it means to "counteract" a condition.[11] Each of the remediation technique examples discussed above makes changes to the device so as to correct a vulnerability. *See* '699 Patent, 5:1-5 ("installation of a patch" or closing a port on a device, changing the device configuration or registry). SecurityProfiling's addition of "counteract" improperly introduces vagueness and ambiguity that is unhelpful to a jury—it suggests that a remediation technique need not actually remediate anything. The extrinsic record, including SecurityProfiling's proffered dictionaries, also supports that "remediation," and related words (*e.g.*, "remedial" or "remedy"), corrects, repairs, or fixes an issue (here, a vulnerability). *See* Ex. 1-J at A163 ("something to correct a wrong"); Ex. 1-K at A168 ("rectify an undesired condition"); Ex. 1-L at A170 ("the correction of something bad or defective"). SecurityProfiling relies on a single non-contemporaneous dictionary to support its addition of "counteract" and it does not warrant adding it to the construction of this term. *See* Ex. 1-M at A174; *see also Jeneric/Pentron*, 205 F.3d at 1380.

[10] This is further shown by the agreed constructions for patch, policy settings, and configuration options (the three remediation types available in the claim and in the specification) which all describe making changes to devices (and/or software running thereon). *See* Joint Claim Construction Statement (Dkt. 88) ("update a computer program to fix a vulnerability"; "device condition established by a policy"; "option for the configuration of a device").

[11] This is true even under SecurityProfiling's construction of "vulnerability" because it is unclear how a weakness, flaw, or gap of a device is "counteracted" as opposed to corrected or fixed.

Once again, SecurityProfiling's vague and overbroad construction likely attempts to expand remediation to unrelated techniques, unintended by the purported invention, such as removal of viruses or other techniques where the vulnerability remains. Accordingly, Trend Micro's succinct and unambiguous construction should be adopted.

E. <u>"patch, policy setting, and configuration option" terms (Claim Terms 5 and 6 – see Ex. 1-A at A9)</u>

Three of the patents include similar terms regarding "patch, policy setting, [and/or] configuration option" types of techniques that can be separated into two different constructions.

1. <u>The '699 Patent includes a "closed" Markush Group</u>

The parties agree that the "patch, policy setting, and configuration option" term in the '699 Patent is a Markush Group, which permits recitation of a list of alternative species that may be selected from a group. However, the parties dispute whether the asserted claim of the '699 Patent may also cover ***other*** remediation technique types beyond those listed. Established Federal Circuit authority mandates that the "consisting of" language within a Markush Group is limiting and makes the group closed. *See Multilayer Stretch Cling Film Holdings, Inc. v. Berry Plastics Corp.*, 831 F.3d 1350, 1358 (Fed. Cir. 2016) (*citing AFG Indus., Inc. v. Cardinal IG Co., Inc.*, 239 F.3d 1239, 1245 (Fed. Cir. 2001) ("the transitional phrase 'consisting of' . . . creates a very strong presumption that that claim element is 'closed' and therefore 'exclude[s] any elements, steps, or ingredients not specified in the claim.'"). Thus, if a patent claim recites "a member selected from the group consisting of A, B, and C," the "member" is presumed to be closed to alternatives D, E, and F. *Id.*; *see also Norian Corp. v. Stryker Corp.*, 363 F.3d 1321, 1331 (Fed. Cir. 2004). Having availed itself of the convenience of Markush claiming, SecurityProfiling cannot now avoid the consequences of that choice under Federal Circuit authority, which requires Trend Micro's construction.

2. <u>The ’708 and ’431 Patents must include each mitigation type</u>

In contrast to the foregoing ’699 Patent claim element, the “patch, policy setting, [and/or] configuration option” terms in the ’708 and ’431 Patents must include each mitigation type. These are not claimed as Markush groups (they lack the key “selected from the group consisting of” language). SecurityProfiling’s repeating the same construction as for the ’699 Patent ignores this differing language. The intrinsic evidence requires the inclusion of mitigation techniques of each recited mitigation type (*i.e.*, the data storage must include at least one technique that is a patch type, one that is a policy setting type, and one that is a configuration option type).

District courts have typically followed *SuperGuide*, interpreting claims reciting “at least one of A, B, and C” to mean “at least one of A, at least one of B, and at least one of C,” unless the claims, specification, or prosecution history require otherwise. *SuperGuide Corp. v. DirecTV Enters. Inc.*, 358 F.3d 870, 884–888 (Fed. Cir. 2004) (requiring inclusion of each category in the list); *see also, e.g., Warner Chilcott Co. LLC v. Mylan Inc.*, Nos. 11-6844, -7228, 2013 WL 3336872, at *4-5 (D.N.J. Jul. 2, 2013); *Kickstarter Inc. v. Fan Funded LLC*, No. 11-cv-6909, 2013 WL 214313, at *6–7 (S.D.N.Y. Jan. 18, 2013); *LMT Mercer Group, Inc. v. Maine Ornamental, LLC.*, Nos. 10-cv-4615, 10-cv-6699, 2014 WL 183823, at *26-27 (D.N.J. Jan. 16, 2014). In addition, even where a disjunctive “or” is used instead of the conjunctive “and,” courts have still required a claimed system to have the capability of all listed options. *See Ameranth, Inc. v. Menusoft Systems Corp.*, No. 2–07–cv–271, 2010 WL 1610079, *6-7 (E.D. Tex. Apr. 21, 2010) (holding that use of disjunctive “or” still required apparatus to be capable of performing both options separated by the “or”). This is consistent with Trend Micro’s construction.

Trend Micro’s construction is also confirmed by the specification, which emphasizes “multi-path remediation”—the ability to offer different types of remediation—as the purported invention. *See e.g.*, ’431 Patent (entitled “Computer Program Product and Apparatus for Multi-

Path Remediation); ’708 Patent (entitled “Multi-Path Remediation).[12] Without the differing types of techniques required under Trend Micro’s construction, multi-path remediation would not be supported by the claims because SecurityProfiling’s broad construction (which mirrors its construction for the Markush Group) permits, for example, a system of all patches. Accordingly, such a construction could exclude the preferred embodiment as well as the purported invention.

3. The ’708 and ’431 Patents are indefinite as it is unclear how patch/policy/configuration types can also be firewall/IPS techniques

Claim 18 of the ’708 Patent and claims 7 and 15 of the ’431 Patent are invalid as indefinite because they require a mitigation technique to be both (1) a type of patch, policy setting, or configuration option and (2) a firewall and/or intrusion prevention mitigation technique. Nothing in the specification suggests a mitigation technique can be both a firewall or IPS technique and also one of the required types. Within the specification, the patch, policy setting, and configuration option types are described as separate techniques or functions from firewalls and IPSs. *See, e.g.*, 19:34-37.[13] Accordingly, the patents fail to inform with reasonable certainty those skilled in the art about the scope of the invention and are therefore indefinite.

F. “occurrence,” “occurrence packet,” and “attack” (Claim Terms 7-9 – see Ex. 1-A at A9)

The parties agree that “occurrence” and “attack” are treated the same in the claims and should be construed identically. Likewise, the parties agree that “occurrence packet” is “a packet that is part of an occurrence.” However, the term “occurrence” only appears in the claims and is

[12] *See also* 7:38-40 (“The remediation techniques include software patches, policy settings or changes, and registry settings or changes.”); 4:54-58 (“remediation techniques include the closing of open ports on the device; installation of a patch that is known to correct the vulnerability; changing the device's configuration; stopping, disabling, or removing services; setting or modifying policies; and the like.”).

[13] The parties’ agreed constructions for “patch,” “policy setting,” and “configuration option” further omit any relation to or indication of firewalls or IPSs.

never used elsewhere in the specification. Therefore, the usage of "attack" in the specification informs the meaning of "occurrence" in the claims. Similarly, due to their identical usage, the recitations of "occurrence" in the claims should guide the construction of "attack" as well. *See Rambus*, 694 F.3d at 48; *Omega Eng'g*, 334 F.3d at 1334.

First, it is clear that the claimed occurrences and attacks are directed to one or more devices and not a computer network as a whole, as suggested by SecurityProfiling. *See, e.g.*, '644 Patent, Claim 1 ("identifying an occurrence in connection with at least one of the plurality of devices"); '431 Patent, Claim 1 ("identifying an attack in connection with the at least one device"); '069 Patent, Claim 2 ("identifying: in connection with the at least one networked device, a first occurrence including at least one first occurrence packet directed to the at least one networked device"). On this ground alone, SecurityProfiling's construction should be rejected.

Second, the claims also make clear that the "occurrence" and "attack" necessarily are "malicious packets" in "network traffic." For example, Claim 2 of the '069 Patent establishes that an "occurrence includ[es] at least one . . . occurrence packet directed to the at least one networked device" (*i.e.*, from network traffic), which is monitored and prevented by the chosen mitigation technique. *See* '069 Patent, Claim 2. The remaining patents that recite "occurrence" are consistent. *See* '644 Patent, Claims 2 and 3; '686 Patent, Claims 4 and 13; *see also Rambus*, 694 F.3d at 48; *Omega Eng'g*, 334 F.3d at 1334. In addition, the specification similarly describes that attacks and occurrences are detected in network traffic (necessarily requiring packets) and blocked by firewall and IPS security systems. *See* 4:18-21 ("firewall 133 drops or rejects the connection request 211 as is understood in the art"); 20:4-9 ("[A]n IPS in-line sensor monitors and processes network traffic" and "the in-line Sensor is commanded in real-time to drop the malicious packets."); *see also GPNE*, 830 F.3d at 1370; *VirnetX*, 767 F.3d at 1318.

SecurityProfiling attempts to improperly broaden the claims with a confusing and ambiguous construction that appears to list different forms of a generic attack. SecurityProfiling bases its construction on extrinsic evidence from Wikipedia and other online sources that do not appear to be contemporaneous with the invention. *See Jeneric/Pentron*, 205 F.3d at 1380; *Brookhill-Wilk 1*, 334 F.3d at 1299. SecurityProfiling's extrinsic evidence from "thefreedictionary.com" supports Trend Micro's construction, as it explains that computer network attacks (as opposed to any generic attack) relies upon packets within network traffic. *See* Ex. 1-N at A191 ("[Computer network attack] relies on the data stream to execute the attack"). SecurityProfiling's construction solely relies on dictionary definitions without reference to the claims or specification and should be rejected.

V. **CLAIM TERMS GOVERNED BY 35 U.S.C. § 112, ¶ 6**

The Court's resolution of a common, threshold question of whether the "code for" and similar terms are means-plus-function limitations governed by § 112, ¶ 6 stands to dispose of five of six Patents-in-Suit and all but one asserted claim in the case. The Federal Circuit requires an algorithm as corresponding structure for computer-implemented means-plus-function limitations and SecurityProfiling does not and cannot point to any algorithms in the specification.

Sitting *en banc* in *Williamson*, the Federal Circuit did away with the strong presumption against § 112, ¶ 6 for terms that lack the word "means," finding it "unjustified." 792 F.3d at 1349. Instead, the question is whether a claim limitation fails to "recite sufficiently definite structure" or recites a "function without reciting sufficient structure for performing that function." *Id.* (citations omitted). Where this is the case, a term is to be construed as a means-plus-function limitation and is limited to the corresponding structure in the specification linked to performance of the claimed function. *Id.* "[D]efining the structure turns on what is recited in the written description, clearly linked to the stated function, and necessary to perform that function." *Harris Corp. v. Ericsson Inc.*, 417 F.3d 1241, 1264 (Fed. Cir. 2005).

Where a means-plus-function element is computer-implemented (like each element here), disclosure of generic computing hardware or software to perform a function is insufficient structure, as it would result in purely functional claiming. Federal Circuit authority "restricts computer-implemented means-plus-function terms to the algorithm disclosed in the specification. . . . A computer-implemented means-plus-function term is limited to the corresponding structure . . . and the corresponding structure is the algorithm." *Id.* at 1253. While an algorithm may be described "in prose," it still must provide "a step-by-step procedure for accomplishing a given result." *Typhoon Touch Tech., Inc. v. Dell, Inc. et al.*, 659 F.3d 1376, 1385 (Fed. Cir. 2011) (citation omitted). Because the algorithm executed by a computer is the necessary structure, a patent that fails to disclose an algorithm and clearly link it to the performance of a claimed function lacks sufficient structure and the claim is invalid as indefinite. *Blackboard*, 574 F.3d at 1384; *see also Williamson*, 792 F.3d at 1352. The requirement to disclose particular structure and clearly link it to a function is the *quid pro quo* a patentee must pay for the convenience of functional claiming under § 112, ¶ 6 and ensure claims are tied to particular structure for implementing an invention. *Noah Sys. Inc. v. Intuit Inc.*, 675 F.3d 1302, 1318 (Fed. Cir. 2012).

A. The "code" terms are governed by § 112, ¶ 6

The asserted claims of the '644, '069, '686, and '431 Patents include elements that merely recite "code for" performing or "code that" performs a function. These unadorned "code for" and "code that" do not provide sufficiently definite structure for performing their recited functions. The number and variety of claimed functions performed by "code" illustrates that the term is nothing more than a generic placeholder and is simply a nonce word in place of "means." The Federal Circuit has held such terms are subject to § 112, ¶ 6. *Williamson*, 792 F.3d at 1350.

The "code" terms here are written in the same format as a traditional means-plus-function limitation, merely replacing the words "means for" with "code for" or "code that" and reciting a function performed by the "code." As with "module" in *Williamson*, the term "code" denotes no more structure than the word "means," and simply serves as a black box to perform the specified function. *Williamson*, 792 F.3d at 1350; *see also Robert Bosch, LLC v. Snap-On Inc.*, 769 F.3d 1094, 1099 (Fed. Cir. 2014) (a term that "refers only to a general category of whatever may perform specified functions" does not identify sufficient structure to avoid § 112, ¶ 6).

District courts, relying on *Williamson*, have held that terms similar to, and arguably even more descriptive than, "code" were governed by § 112, ¶ 6. In *Zeroclick LLC v. Apple Inc.*, the court held that claim limitations reciting the terms "program" and "user interface code" were governed by § 112, ¶ 6. No. 15-cv-04417-JST, 2016 WL 5477115 at *4–*6 (N.D. Cal. August 16, 2016) (holding that the claim terms "program that can operate …" and "user interface code" did not "recite any structure whatsoever, let alone 'sufficiently definite structure.'" citing *Williamson*, 792 F.3d at 1349; *id.* at 1351–52). Similarly, in *Verint Sys. Inc.*, the court found the term "first computer application" to be governed by § 112, ¶ 6. *Verint Sys. Inc. v. Red Box Recorders Ltd.*, 166 F. Supp. 3d 364, 379-80 (S.D.N.Y. 2016) (holding that even considering the proffered dictionary definition of "application" as "[a] collection of software components used to perform specific types of user-oriented work on a computer," the term "fails to provide sufficient additional structure"). Here, for at least the reasons recognized by the *Zeroclick* and *Verint* courts, the term "code" does not recite sufficiently definite structure to perform the recited functions.[14] Because the "code" limitations are drafted in functional terms, without reciting any

[14] The "code" terms constitute most, and in many cases all, of the claims' limitations. Thus, the claims do "not describe how the [term] interacts with other components . . . in a way that might inform the structural character of the limitation-in-question or otherwise impart structure to the"

structure that would distinguish the claimed "code" from a general purpose computer program, the claim terms are governed by § 112, ¶ 6.

B. The additional "nonce" terms are similarly governed by § 112, ¶6

In addition to the "code" terms, the '686,'708, and '431 Patents include additional nonce terms that should likewise be governed by § 112, ¶ 6. Particularly, the claims include terms such as "processor," "data storage," and "component" that perform particular functions. Like *Williamson* and the "code" terms, these terms are mere "generic description[s] for software . . . that performs a specified function." *See* 792 F.3d at 1350; *see also, e.g.*, *Advanced Ground Info. Sys., Inc. v. Life360, Inc.*, 830 F.3d 1341, 1347 (Fed. Cir. 2016) (construing "symbol generator"); *Media Rights Techs., Inc. v. Capital One Fin. Corp.*, 800 F.3d 1366, 1373-74 (Fed. Cir. 2015) ("compliance mechanism"); *Farstone Tech., Inc. v. Apple Inc.*, No. 8:13-cv-1537, 2015 WL 5898273, at *4-5 (C.D. Cal. Oct. 8, 2015) ("backup/recovery module").

While the "component" terms do include modifiers such as "intrusion prevention system component" and "firewall occurrence mitigation system component," these descriptors merely further describe the broad recited functions and do not provide any further indication as to the structure of the component or the software it represents. *See, e.g.*, *Robert Bosch*, 769 F.3d at 1099-101 (terms "program recognition device" and "program loading device" subject to § 112 ¶ 6 because the prefixes merely identify functions of the "device"); *Williamson*, 792 F.3d at 1351–52 (construing "distributed learning control module"). For example, it is unclear if the firewall component is an entire firewall, one small aspect of a firewall, or firewall functionality of some

term). *See Williamson*, 792 F.3d at 1351–52 (construing "distributed learning control module"); *see also Global Equity Management (SA) Pty. Ltd. v. Expedia, Inc.*, No. 16-CV-95-RWS-RSP, 2016 WL 7416132, at *29-30 (E.D. Tex. Dec. 22, 2016) ("the program code is defined only by the function that it performs").

other application.[15] Further, the asserted claims do not describe how the claimed nonce terms interacts with other components in each of the claims other than being generally "communicatively coupled" to other components. *See Williamson*, 792 F.3d at 1351–52.

C. **The "code" and other nonce terms are indefinite because the specification fails to disclose clearly linked structure to perform each claimed function**

As discussed below, each limitation governed by § 112, ¶ 6 is indefinite because the specification fails to provide an algorithm that performs the recited functions. For § 112, ¶ 6 the usage of nonce terms like "code" (and the claims' other nonce terms) connotes software, which necessarily requires disclosure of an algorithm. *See, e.g.*, *Blackboard*, 574 F.3d at 1385.[16] Given the strict requirements of § 112, ¶ 6 and the "quid pro quo" required for functional claiming, the specification of the Patents-in-Suit is lacking. *See Noah Sys*, 675 F.3d at 1318.

Indeed, SecurityProfiling does not—and cannot—point to particular algorithms for the claimed functions in the specification, let alone ones clearly linked to those functions. Thus, if these elements require an algorithm, it is clear the claims are indefinite. This lack of disclosure is a natural result of the Patents-in-Suit issuing from disclosures taken practically verbatim from product marketing materials, which are repetitive and fail to provide any detail regarding the

[15] Additionally, for the '708 Patent, the "intrusion prevention system component" is merely one "component" of the claimed intrusion prevention system. *See* '708 Patent, Claim 18. Accordingly, the "intrusion prevention system" modifier provides no help in distinguishing the structure of the "system" from the "system component" thereof.

[16] The requirement of an algorithm is particularly applicable here, where the specification confirms that the "code" and other nonce terms are implemented in programming executed by generic, general purpose hardware. *See, e.g.*, 2:29-32 ("In particular, security server 135 includes processor 142, and memory 144 encoded with programming instructions executable by processor 142 to perform several important security-related functions."); 3:12-58 ("processor 142, 152, 162 are of a conventional, integrated circuit microprocessor arrangement . . . ."); *see also Blackboard*, 574 F.3d at 1385 ("The correct inquiry is to look at the disclosure of the patent and determine if one of skill in the art would have understood that disclosure to encompass software for [performing the recited function] and been able to implement such a program, not simply whether one of skill in the art would have been able to write such a software program.").

structure or algorithms for the claimed inventions. As a result, the specification fails to provide any detailed flowcharts, diagrams, or specific sets of instructions sufficient to satisfy the numerous functions recited in the claims. Thus, given this lack of disclosure, each of the asserted claims in the ’644, ’069, ’686, ’431, and ’708 Patents should be rendered indefinite.

1. **Claim Terms Concerning Multiple Mitigation Techniques (Claim Terms 10-23 – see Ex. 1-A at A9 – A17)**

The specification fails to disclose a clearly linked and sufficiently definite algorithm describing *how* the claimed “code” or “processor” is configured to perform the claimed functions concerning multiple mitigation techniques. *See Blackboard*, 574 F.3d at 1384 (algorithm must describe “how the [means] ensures that those functions are performed,” not merely an intended outcome). Terms 10-23[17] from the ’644, ’069, ’431, and ’686 Patents recite functions for the display of multiple mitigation techniques, including firewall and IPS options, receiving user input regarding those techniques, and applying them. The parties generally agree on the functions for the limitations in this group but dispute the required structure or algorithm.

As a threshold matter, none of the figures or detailed description discloses anything regarding presenting both firewall and IPS techniques as alternatives. The core of these functions requires the display of multiple mitigation techniques, and the specification only briefly discusses firewalls and IPSs in separate embodiments. *See, e.g.*, 13:37-45 (firewall embodiment); 19:8-36 (IPS embodiment). This lack of a corresponding algorithm is further highlighted by SecurityProfiling’s “alternative” structure, which primarily points to Figures that consist of black-box computers, processors, databases, and servers. The closest components that

[17] The parties have agreed on seven groupings of the mean-plus-function terms based on common subject matter as presented in the Joint Claim Construction Statement and Exhibit 1-A hereto. The groupings reflect common issues for related terms and are drawn to reduce the number of questions for the Court. As shown in Exhibit1-A, Trend Micro contends that construction of a few representative terms should resolve the questions for each term in the groupings.

SecurityProfiling points to that could provide a user-interface necessary to perform the claims, are a generic "Management Console(s) 803" and "IPS Console." *See* Figures 1, 2, 8, and 11. However, these generic network figures do not provide a step-by-step procedure for achieving the recited functions and merely depict generic computers and processors. *See Aristocrat Techs. Austl. Pty Ltd. v. Int'l Game Tech.*, 521 F.3d 1328, 1336 (Fed. Cir. 2008) (general purpose computer with "appropriate programming" is insufficient disclosure under 112, ¶ 6).

The specification provides no discussion, let alone an algorithm, for how: (a) mitigation techniques using firewalls or intrusion prevention systems (or any others) are presented or displayed to the user; (b) a user may configure those mitigation techniques; or (c) the user selects the mitigation techniques. Indeed, the specification does not describe ***any*** user interactions during the operation of the firewall or IPS. *See* 4:13-21 ("Security server 135 sends result signal 217 back to firewall 131 with an indication of whether the connection request should be granted or rejected. . . . [S]ignal 217 indicates that connection request 211 is to be rejected, firewall 133 drops or rejects the connection request 211 as is understood in the art.");[18] 20:4-9 ("[I]f the destination IP is vulnerable to the attack, the in-line Sensor is commanded in real-time to drop the malicious packets").

Other than generic network figures, SecurityProfiling also points to 4:41-53, 5:36-6:16. At best these passages are limited to remediation techniques (*i.e.*, patches, policy settings, and configuration options) and not mitigation techniques utilizing firewalls or IPSs. Rather, the remediation techniques discussed by the specification for fixing a device vulnerability are distinct from the firewall or IPS prevention of an attack. *See, e.g.*, 19:34-37 ("[I]f the destination

[18] Referring to what is "understood in the art" does not disclose an algorithm under § 112, ¶ 6. *See Triton Tech of Tex., LLC v. Nintendo of Am., Inc.*, 753 F.3d 1375, 1378 (Fed. Cir. 2014) ("[a] bare statement that known techniques or methods can be used does not disclose structure").

IP is vulnerable to the attack, the in-line Sensor is commanded to immediately drop the exploit packets—preventing the attack. Further, it remotely remediates the vulnerability" by "deploy[ing] the appropriate update to the machine or device . . . ."). This is not an algorithm clearly linked to the claimed functions. Regardless, the proffered "structure" and/or "algorithm" do not provide a step-by-step procedure for achieving the recited functions and is neither clearly linked to nor sufficient to perform the claimed functions regarding the firewall and IPS. *See Blackboard*, 574 F.3d at 1385. Because the specification discloses no algorithm for achieving the recited functions, these terms are indefinite and the corresponding claims are invalid.

2. <u>Claim Terms for Updating a Firewall and an Intrusion Prevention System (Claim Terms 24-29 – see Ex. 1-A at A17 – A20)</u>

Similar to the functions for multiple mitigation techniques, the specification also fails to disclose a particular algorithm for *how* the claimed "code" or "component" is configured to perform the functions concerning updating a firewall and an IPS. Terms 24-29 from the '686 Patent concern receiving user input following the display of options, sending an appropriate rule or update to the firewall and to the IPS, and receiving the rule or update by the firewall and IPS.

Again, SecurityProfiling provides an "alternative" structure which only points to Figures that consist of a black-box of network components with generic consoles. These do not provide a step-by-step algorithm for achieving the recited functions; indeed, they lack description of the functions' user interface for updating firewalls and IPSs altogether. *See Aristocrat*, 521 F.3d at 1336. Moreover, the cited specification includes no discussion of sending updates and rules to a firewall and an intrusion prevention system. SecurityProfiling does not provide any additional specification support for its alternative structure or algorithm. Nor can it. While the specification does state that "one possible embodiment may also provide product upgrades and signature updates to each of these various security products—including all of the technology benefits such as ensuring compliance of signature versions, logging, reporting, and verification of installation," 14:35-39, this does not approach a step-by-step algorithm that is sufficient to perform or clearly linked to the claimed functions as required to satisfy Section 112, ¶ 6. *See Blackboard*, 574 F.3d at 1385; *Aristocrat*, 521 F.3d at 1334 (such language merely "describes an outcome, not a means for achieving that outcome").

3. **Claim Terms Concerning Identifying an Occurrence in Connection with a Device (Claim Terms 30-31 - see Ex. 1-A at A20 – A21)**

The specification fails to disclose or clearly link a particular algorithm describing *how* the claimed "code" performs the functions concerning identifying an occurrence in connection with a device. In particular, Terms 30-31 from the '644 and '069 Patents, primarily concern the identification of one or more occurrences and occurrence packets.

As above, SecurityProfiling again provides an "alternative" structure which only points to Figures that consist of a black-box network infrastructure, do not provide algorithms, and lack any description of ***how*** any component identifies one or more occurrences and occurrence packets.[19] *See Aristocrat*, 521 F.3d at 1336. The specification suggests that these functions ***should be*** performed (*see, e.g.*, 3:59-65, 20:4-5), but includes no step-by-step procedures for achieving the recited functions nor any algorithm or detail as to ***how*** they might be performed, such as how the claimed code processes network traffic, identifies relevant packets, or determines that the traffic is an occurrence rather than benign data. *See Blackboard*, 574 F.3d at 1385; *Augme Techs., Inc. v. Yahoo! Inc.*, 755 F.3d 1326, 1338 (Fed. Cir. 2014) ("Simply disclosing a black box that performs the recited function is not a sufficient explanation of the

[19] SecurityProfiling includes citations to "Attacker 115" and "Internet 120" of Figure 1 for these limitations (and others), which clearly cannot be part of the structure of or algorithm performed by the "computer program product" or "apparatus" claims of the Patents-in-Suit.

algorithm required to render the means-plus-function term definite."). These terms are indefinite and the corresponding claims are invalid.

4. <u>Claim Terms for Determining Whether Devices Are Actually Vulnerable to an Occurrence or Attack (Clam Terms 32-35 – see 1-A at A21 – A23)</u>

Similar to the preceding functions for identifying occurences, the specification fails to disclose a particular algorithm describing *how* the claimed "code" performs the claimed functions concerning determining whether devices are actually vulnerable to occurrences or attacks. In particular, Terms 32-35 from the '644, '069, and '431 Patents primarily concern the determination of whether one or more devices is vulnerable to one or more detected attacks or occurrences using information about the devices, including actual vulnerability information.

As above, SecurityProfiling provides an "alternative" structure which only points to Figures that consist of a black-box network infrastructure and do not provide an algorithm for determining whether one or more devices are actually vulnerable to one or more occurrences or attacks. *See Aristocrat*, 521 F.3d at 1336. Moreover, there are no algorithms in the specification, such as through flow charts or diagrams, on where the claimed code is located or how the claimed code accesses the vulnerability information and uses that information to determine whether a device is actually vulnerable (or not vulnerable) to an identified occurrence or attack. While the specification might provide examples of particular determinations such as a firewall that "sends a query 213 to security server 135" (3:59-4:12) or that "an IPS in-line sensor . . . sends real time alert data to the on-site server where it cross-references the data with the backend" (20:4-6), these examples merely reference an intended outcome and do not provide a step-by-step procedure for how such outcomes are achieved, let alone one that is clearly-linked to the recited functions. *See Blackboard*, 574 F.3d at 1384-85; *Augme*, 755 F.3d at 1338. In addition, the claim limitations use open-ended language, including "at least one of the plurality of devices," "at least one vulnerability," and/or require determinations of multiple occurrences. But the specification does not provide an algorithm for this open-ended language requiring multiple determinations involving multiple occurrences, devices, and vulnerabilities.

5. Claim Terms Concerning Storing Information Associated with Multiple Actual Vulnerabilities (Claim Terms 36-37 – see Ex. 1-A at A23 – A24)

The specification fails to disclose a sufficiently definite algorithm describing *how* the claimed "code" performs the claimed functions concerning storing information associated with multiple actual vulnerabilities. In particular, Terms 36-37 from the '686 Patent primarily concern creation and storage of information associated with actual vulnerabilities, derived from potential vulnerability information and operating systems and applications information.

As discussed above, SecurityProfiling provides an "alternative" structure which only points to Figures that consist of a black-box network infrastructure, do not provide algorithms, and lack any description of creation and subsequent storage of actual vulnerability information in a data storage (as opposed to storage of potential vulnerability information and device information). *See Aristocrat*, 521 F.3d at 1336. Moreover, there are no algorithms in the specification that provide step-by-step procedures for achieving the recited functions, such as through flow charts or diagrams. Indeed, the specification does not disclose the storing of actual vulnerability information for devices on a network in a "data storage" at all. While the specification provides examples of data storage, such as a "security server," that do receive and store various information in order to "perform several important security-related functions" (2:29-3:10; 3:12-26), none provide a step-by-step procedure for achieving the recited functions, let alone clearly links such disclosures to those functions. *See Blackboard*, 574 F.3d at 1385; *Augme*, 755 F.3d at 1338. These terms are indefinite and the corresponding claims are invalid.

6. **Claim Terms Concerning Data Storage of Device and Vulnerability Information (Claim Terms 38-42 – see Ex. 1-A at A24 – A27)**

The patent specification fails to disclose a particular algorithm describing *how* the claimed software performs the claimed functions concerning accessing and receiving information associated with multiple actual vulnerabilities and/or mitigation techniques. In particular, Terms 38-42 from the ’644, ’069, ’431,’686, and ’708 Patents, primarily concern access and retrieval of stored information associated with actual vulnerabilities, which is derived from potential vulnerability information and information regarding various devices and/or mitigation techniques for mitigating effects of attacks that take advantage of vulnerabilities.

As above, SecurityProfiling provides an “alternative” structure which only points to Figures that consist of a black-box network infrastructure, do not provide step-by-step algorithms, and lack any detail for how the claimed derivation, storage, and access of actual vulnerability information and/or mitigation techniques are performed. *See Aristocrat*, 521 F.3d at 1336. Moreover, there are no step-by-step procedures in the specification for how the claimed functions are achieved. For example, there is no algorithm disclosed for how firewall and IPS mitigation techniques are to be associated with a particular vulnerability or occurrence in a data storage. While the specification might provide examples of data storage, such as a “security server” that generally receives and stores various information in order to “perform several important security-related functions” (2:29-3:10; 3:12-26), at best, these describe intended outcomes but do not provide a step-by-step procedure showing how the recited functions are achieved, let alone one the specification clearly links to those functions. *See Blackboard*, 574 F.3d at 1385; *Augme*, 755 F.3d at 1338.

Thus, the claim terms are indefinite, and the corresponding claims are invalid.

7. **Additional Claim Terms (Claim Terms 43-45 – see Ex. 1-A at A28 – A29)**

The specification fails to disclose a sufficiently definite algorithm describing *how* the claimed "code" performs the claimed functions concerning the various additional Terms 43-45 that only appear in the '069 Patent, including reporting an occurrence that is capable of taking advantage of an actual vulnerability on one more device in Term 43, which is exemplary.

As above, SecurityProfiling proposes an "alternative" structure which only points to Figures that consist of a black-box network infrastructure, does not provide step-by-step algorithms, and lacks any description of the claimed reporting (among other things). *See Aristocrat*, 521 F.3d at 1336. Moreover, there are no step-by-step procedures in the specification for how the recited functions are achieved, including, for example, where the claimed code is located or how the claimed code handles the claimed reporting, determines what to report, and displays or otherwise reports the claimed occurrence to a user. While the specification provides general examples of logging or otherwise tracking data,[20] these examples do not report that devices are actually vulnerable to an occurrence and, regardless, do not provide a step-by-step procedure for achieving the recited functions, let alone clearly links such disclosures to the claimed functions. *See Blackboard*, 574 F.3d at 1385; *Augme*, 755 F.3d at 1338.

Thus, the claim terms are indefinite, and the corresponding claims are invalid.

[20] For example, SecurityProfiling's LogBoss embodiment only discusses logging information generally and is not clearly linked to the recited function. reporting occurrences. *See* 16:60-17:16. In addition, the IPS embodiment references "real time alert data," but this is (a) outputted to a security server, not reported and (b) does not include data about whether an occurrence can take advantage of an actual vulnerability as required by the claimed function, as this vulnerability determination is made later based on further processing after the alert. *See* 20:4-9.

Dated: January 11, 2018

Respectfully submitted,

By: */s/ Yar R. Chaikovsky*
Yar R. Chaikovsky, CA Bar No. 175421
yarchaikovsky@paulhastings.com
Michael C. Hendershot, CA Bar No. 211830
michaelhendershot@paulhastings.com
Evan M. McLean, CA Bar No. 280660
evanmclean@paulhastings.com
PAUL HASTINGS LLP
1117 S. California Ave.
Palo Alto, California 94304-1106
Telephone: (650) 320-1800
Facsimile: (650) 320-1900

E. Leon Carter, Bar No. 03914300
Scott W. Breedlove, Bar No. 00790361
CARTER SCHOLER, PLLC
8150 N. Central ExpY., Suite 500
Dallas, Texas 75206
Telephone: (214) 550-8188
Facsimile: (214) 550-8185
Email: lcarter@carterscholer.com
Email: sbreedlove@carterscholer.com

Attorneys for Defendants Trend Micro America, Inc. and Trend Micro, Inc.

CERTIFICATE OF SERVICE

The undersigned certifies that the foregoing document was filed electronically in compliance with Local Rule 5.1(d). As such, this document was served on all counsel who are registered users of ECF on this 11th day of January, 2018.

By: */s/ Yar R. Chaikovsky*
Yar R. Chaikovsky